

SECURING ACCESS BETWEEN CORPORATE LOCATIONS

After reading this chapter and completing the exercises you will be able to:

- ◆ Identify the security risks that exist for information passing between corporate locations.
- ◆ Implement and secure Windows 2000 when it is configured as a router.
- ◆ Implement and secure Windows 2000 when it is configured as a Virtual Private Network server.
- ◆ Secure network access for partner organizations.

Most large companies have more than one location. These sites may be located throughout a city, a country, or the world. In most cases, these remote locations must be able to communicate with other corporate locations. Often the company may want to share resources efficiently and securely across all locations. For example, Lonestar Graphics may have its corporate office in Winnipeg, but have distribution centers in Toronto and Vancouver. There may be a need to share information, such as inventory or accounting data, between the three locations. The data that is to be transmitted between the remote locations must be secure from unauthorized access or tampering. As you design your security plan, you will need to make sure that the data sent between company locations is secure.

Security is also a major concern to a company that shares information with partner organizations. Two companies may decide to form a partnership to complete a large project. Information such as inventory, design plans, and other project-related material stored at one company's location may have to be available to both companies. In this scenario you may have to ensure that users from both companies can access the appropriate shared information, but that they are also restricted from accessing unauthorized areas within each other's network. As well, user authentication and the transmission of data between the two companies has to be secure and reliable.

This chapter discusses various methods of securing the connections between a corporate office and remote locations or partner organizations. A Windows 2000 server can be configured as a router to enable the routing of information across network links to remote locations. This router may be set up and configured to use a static connection to locations that have persistent connections. For locations that require a dial-up connection, the Windows 2000 router can also be configured as a demand-dial router.

Some remote locations may access the corporate network through the Internet. For these types of connections, a Virtual Private Network (VPN) can be configured to enable a secure and protected virtual tunnel through the Internet. If you are implementing a VPN solution as part of your security plan, you will have to decide what type of VPN to implement, and what authentication and encryption protocols you will use to create the VPN tunnel.

The final topic in the chapter discusses the process of securing the collaboration and sharing of information between partner organizations. This includes various methods of securing resource access, data transmission, and authentication to the remote network.

SECURITY RISKS FOR DATA BETWEEN CORPORATE LOCATIONS

Companies that have multiple locations require an additional level of complexity for their security plan when compared to organizations with only one location. As illustrated in Figure 9-1, the network traffic is no longer restricted within a self-contained network. To enable the sharing of information between all of the remote locations, the data is now transmitted across a wide area network (WAN). Because these connections are outside the office and often outside the direct control of the company, protecting data on the connections presents an extra challenge.

A **wide area network (WAN)** is a network system that connects two or more remote locations over a wide geographical area. This connection is made by using either a private or public network infrastructure.

The **private network infrastructure** may consist of a dial-up connection between the locations, or a persistent connection that is owned and maintained by a service provider and leased by the company. Private networks are considered fairly secure because the infrastructure is not accessible to the general public. One concern is that service providers often lease shared lines to multiple customers. For example, the service provider may lease some of the channels in a T1 connection to multiple clients who need a fractional T1 line. This increases the threat of unauthorized access or viewing of the data transmissions on the network. To ensure that your data is secure in this case, you must make sure that data is protected during transmission and that user authentication is being controlled. These measures will ensure that only authorized users access each remote location.

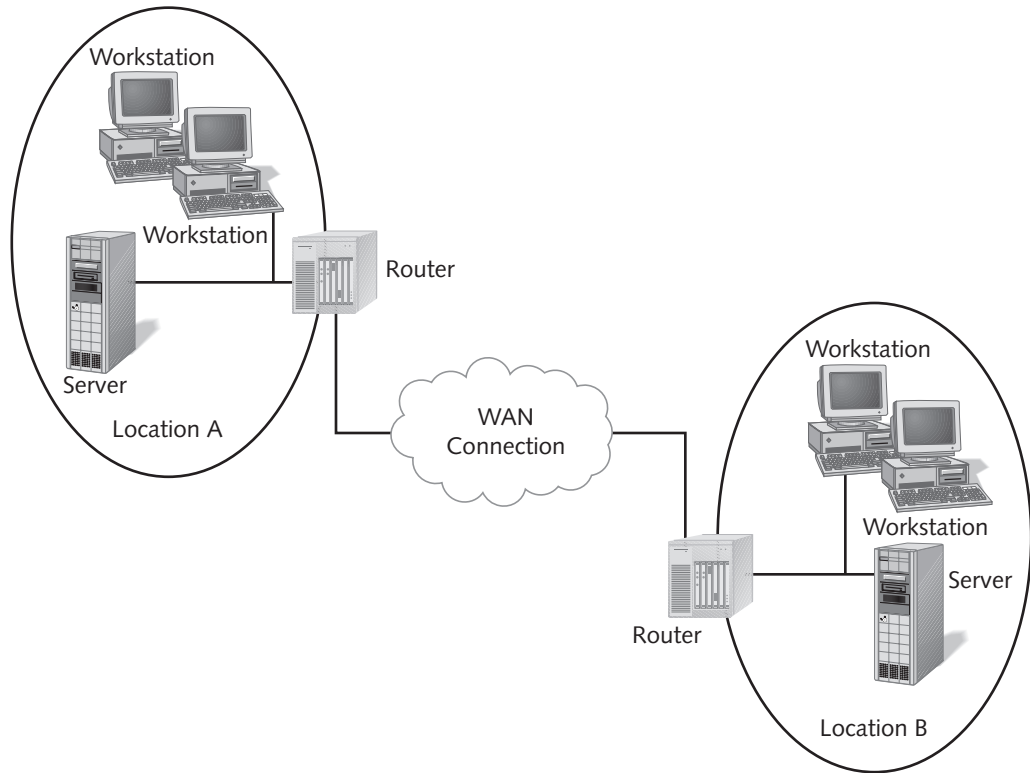


Figure 9-1 Corporate locations connected by a WAN link

The main advantage to using a leased line is that bandwidth and availability is usually more reliable and controlled. The access and bandwidth control comes with a price, however, as leased lines are usually expensive to implement throughout an organization.

The **public network infrastructure** usually incorporates the Internet as a way of connecting the various remote locations. In other words, the Internet becomes the WAN link between corporate locations. The Internet is a much less secure infrastructure because of wide public accessibility, which means that the chance of unauthorized access to the data is greatly increased.

One advantage to using a public network infrastructure is the low cost. The cost of using the Internet as a WAN between remote corporate locations is very reasonable, especially with the advent of cable modem and DSL connections. Often this Internet connection is also much faster than the private network connection. If you are going to use the Internet as a WAN connection, you will need to implement a VPN to establish a virtual tunnel between the locations. This tunnel encrypts and secures the data that is transmitted between the remote locations, even through the Internet.

Regardless of whether a public or private WAN connection is used, several important security risks arise as soon as the data leaves your corporate network. The corporate security plan must include identification of each security risk and outline how each risk will be addressed. Some common risks and solutions include the following:

- *Data integrity*—Administrators have to be sure that as data is transmitted over the WAN links, there is no chance of data being captured and altered before it reaches its destination. Various security options exist to address this issue. Depending on the connection protocol and method used, the administrator can limit which computers can transmit data across the WAN link. This can be accomplished by configuring packet or routing rules on routers or firewalls. Mutual authentication can also be enabled between computers or routers to limit which points can actually establish communication connections. Another option is to require all messages sent between corporate locations to be digitally signed before they are sent.
- *Data confidentiality*—As data is transmitted through the WAN connections, it can be captured and viewed by unauthorized users. To combat this security risk, routers or computers can be configured to encrypt the data between the various remote locations. IP Security (IPSec) is one technology that can be used to encrypt data between corporate locations. (For more information on IP Security look at Chapter 7, “Securing Network Communications.”)
- *User resource authentication*—Securing resources that are accessible through external networks is another important task for the administrator. Special applications, such as messaging and Web servers or terminal services, can potentially allow access into private network systems if not correctly secured and controlled. The implementation of firewall configurations, such as screened subnets or demilitarized zones (DMZs), may help in controlling access to applications, resources, or private network systems. Screened subnets are discussed further in Chapter 10, “Designing Secure Access to the Internet.” A Public Key Infrastructure can also be implemented to assist in the authentication and mapping between business partners and internal user accounts to give access to internal resources. Chapter 5, “Implementing a Public Key Infrastructure” discusses PKI in more detail.

If you are going to use Windows 2000 to secure WAN communications, you can use the service included with Routing and Remote Access. RRAS can be configured to provide security in a number of scenarios, including private network scenarios, and virtual private networking across public networks.

Routing and Remote Access Services (RRAS) consists of several subservices incorporated into one utility. In addition to dial-up remote access support, RRAS includes the following:

- Persistent and demand-dial multiprotocol router
- Virtual Private Networking (VPN) support

- RADIUS Client Support
- Network Address Translation (NAT)

The sections that follow will expand on the router and VPN capabilities of RRAS.

CONFIGURING WINDOWS 2000 AS A ROUTER

Some companies that have multiple geographically distributed locations connect these locations using dedicated, private connections. These dedicated links are connected to the local network by using a router. A **router** is a networking device, either software-based or hardware-based, that controls and forwards packets between networks. A hardware-based router is a device that is dedicated to the tasks of forwarding, securing, and analyzing packets. As a cost-effective alternative, Windows 2000 includes a router as part of the RRAS service. This software-based router provides many of the same features of its hardware-based counterparts, but at a lower cost of implementation. Although not generally recommended as a replacement to a high-performance dedicated router, this router's performance is sufficient to support a small to medium-sized corporate LAN connected to another LAN or remote WAN.

A router acts as a gateway from one network to another. The router has two network adapters, each connected to a different network segment. When a packet arrives at one of the network adapters, the router examines the destination address for the packet. If the destination address is on the network that is attached to the other network adapter, the router passes the packet to that network adapter and out on to the network. A slightly more complicated router scenario occurs if the company has two locations that are connected with a T1 WAN connection. Each location requires that a router listen for network traffic destined for the address of a computer on the other network. The router forwards the traffic across the T1 line to the router at the other location. The router in the destination location will then forward the packet to the correct computer.

Routers are also used in more complicated scenarios. A company can have hundreds of locations connected by a variety of WAN links. Some of the links may be VPN connections through the Internet connecting the various locations or connecting a dedicated private network connection. Other links may be modems dialing up to a RAS server in a central location. RRAS in Windows 2000 can be used as a router in each of these scenarios.

Configuring Routing Options

The router included with Microsoft Windows 2000 supports a wide range of open Internet standards. This includes support for standard networking protocols, such as Internet Protocol (IP), Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX), and AppleTalk. Windows 2000 RRAS also provides support for several open-standard Internet routing protocols, such as multicasting, Routing Information Protocol (RIP version 1 and version 2), Open Shortest Path First (OSPF), and static routing.

Windows 2000 based routers also support various types of network interfaces such as dial-up modems, Integrated Services Digital Network (ISDN), Asymmetric Digital Subscriber Lines (ADSL), cable modems, and private connection interfaces such as T1 and T3 connections.

Windows 2000 provides the routing functionality through RRAS. RRAS is installed on all Windows 2000 servers by default, but it must be configured before implementation. To configure RRAS as a router, follow the steps below:

1. Click **Routing and Remote Access** from the Administrative tools menu.
2. As shown in Figure 9-2, right-click the server name or choose **Action** and choose **Configure and Enable Routing and Remote Access**.

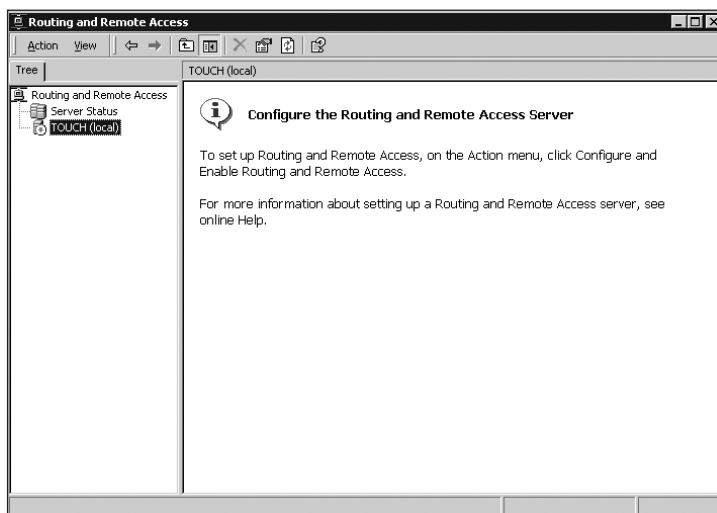


Figure 9-2 Configuring Routing and Remote Access

3. Click **Next** at the RRAS Setup Wizard welcome screen to view the common configurations of RRAS, as shown in Figure 9-3. To configure the routing options, choose **Network router** and click **Next**.
4. Verify that the required protocols are available. If they are not, you will have to exit the Wizard and install the appropriate network protocols before continuing. Click **Next**.
5. As shown in Figure 9-4, the next screen allows the choice of configuring demand-dial routing. If configuring demand-dial routing, choose **Yes**; otherwise choose **No**, and then finish the Wizard.

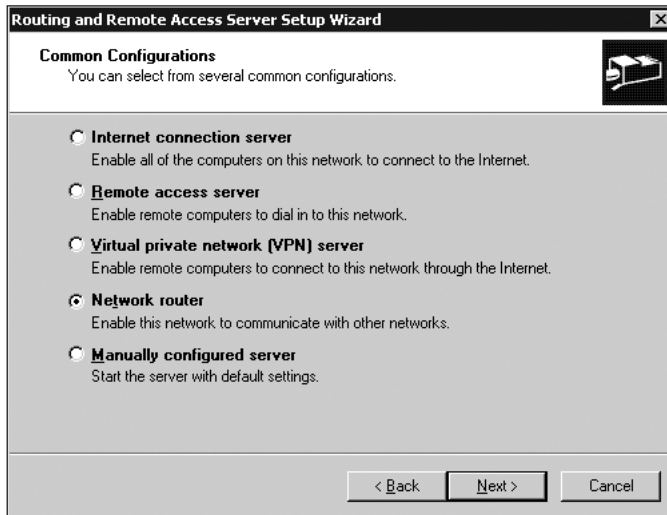


Figure 9-3 Configuration options in RRAS

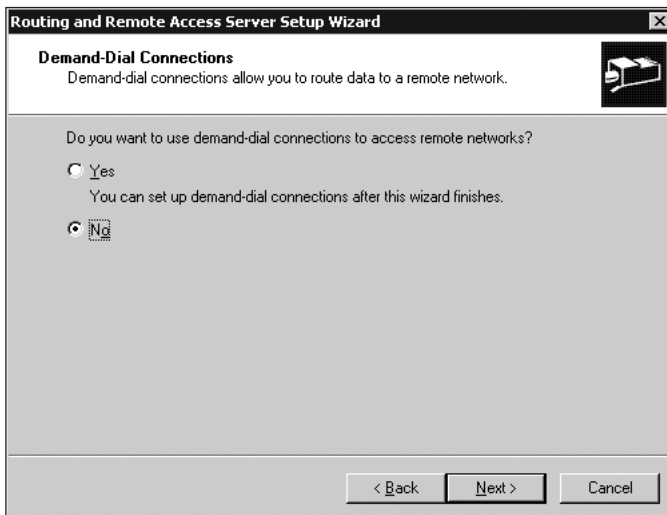


Figure 9-4 Configuring demand-dial routing

6. If demand-dial routing is chosen, the next Wizard allows you to choose how IP addresses will be allocated. Figure 9-5 shows this configuration screen.

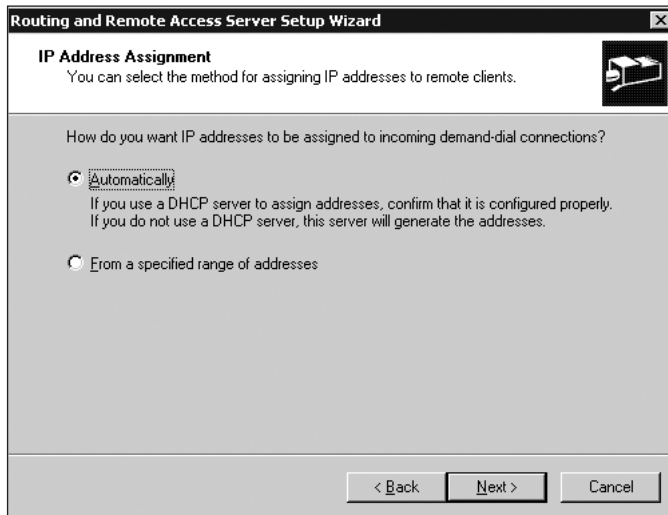


Figure 9-5 Configuring IP address allocation for RRAS

7. The final screen in the RRAS Setup Wizard lists additional configuration settings that should be completed after the Wizard setup and before the server can be used as a router. These additional tasks, as illustrated in Figure 9-6, include adding and configuring the demand-dial interfaces ensuring correct IP address allocations, and installing and configuring routing protocols.



Figure 9-6 Completing the router configuration settings

As illustrated in the previous procedure, the RRAS server can act as a LAN-to-LAN router, demand-dial router, and a VPN router.

LAN-to-LAN Configurations


A LAN-to-LAN configuration assumes that all the LAN segments are available at all times. This configuration is straightforward and requires only a few steps following installation, such as configuring static routes if the LAN is separated into multiple network sections.

When a Windows 2000 server is configured as a router, the router includes a number of routing table entries based upon the network interfaces installed in the machine. A **routing table** is a list of all the networks that a router knows about and the addresses that the router can use to forward messages to that network. This table is used as a map to determine the path for the packets as they are sent between network segments. To view the current routing table on a server, open a command prompt and type route print, or follow the directions below:

1. Open **RRAS** from the **Administrative tools** menu.
2. Expand **IP Routing**.
3. Right-click **Static Routes** and select **Show IP Routing Table**. A sample routing table is illustrated in Figure 9-7.

TOUCH - IP Routing Table					
Destination	Network mask	Gateway	Interface	Metric	Protocol
0.0.0.0	0.0.0.0	192.168.0.1	Network	1	Network management
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.0.0	255.255.255.0	192.168.0.2	Network	1	Local
192.168.0.2	255.255.255.255	127.0.0.1	Loopback	1	Local
224.0.0.0	240.0.0.0	192.168.0.2	Network	1	Local
255.255.255.255	255.255.255.255	192.168.0.2	Network	1	Local

Figure 9-7 Viewing the Routing table on the RRAS server



The routing table includes a number of additional entries, including the default route to the default gateway, loopback address, and multicast addresses. It also contains an extra column called Protocol, which identifies how RRAS determined the route. Local means that the router is directly attached to that network.

By default, Windows 2000 routers are only aware of networks connected directly to the installed network adapters within the computer. For example, if a Windows 2000 router were connected to network segment A and network segment B through two network adapters, the router would be able to direct traffic between the two segments. This is possible because the addresses for both network segments will automatically be listed in the routing table. If a company has multiple locations separated by routers, each network segment that is not directly connected to a router needs to be added to the routing table. For example, segment A may be connected to segment B, and segment C may be connected to segment B. For packets to be able to route from A to C, an entry has to be placed into segment A's routing table that directs packets to segment B first, and then the routers on segment B can forward the packets to segment C. The path to segment A

would have to be configured in the routing tables for the routers in segment C, so that the packets could be routed through B to get to A.

Static routes are routing table entries that are manually entered into the routing table to assist the router in forwarding packets to networks not directly connected to the router. To add a static route to the routing table, follow the procedure below:

1. Click Routing and Remote Access. Open **RRAS** from the Administrative tools menu.
2. Expand the server container and then expand **IP Routing**.
3. Right-click **Static Routes** and select **New Static Route**.
4. Select the Interface through which the packets will be sent and fill in the Destination, Network Mask, Gateway, and Metric fields.
5. Click **OK**.

Configuring the static routes on each router requires considerable administrative effort. As the network begins to include more locations, the administrative effort of managing the static routes can become too high and there may be a greater need for the routers to be able to respond to failed network connections. In addition, routers that have been configured with static routes cannot adjust to changing network conditions. For example, if a network connection fails, the router cannot remove the static routes and choose a different route through the network. Because of this, static routes are usually used only for small companies with less than five locations connected with routers.

In a more complex environment, you must use a **routing protocol**. This is a protocol used by routers to automatically build and maintain the routing tables for a complex network. When a routing protocol is used, each router broadcasts its routing table to the other routers on the network. Each router adds this information to its routing table. When a new route and router are added to the network, this information is automatically spread to all of the existing routers. Using a routing protocol also adds fault tolerance to the network. If a router fails, or if a network link becomes unavailable, this information is added to the routing tables. The routers then use alternative routes around the failed component.

RRAS in Windows 2000 supports two of the most common routing protocols:

- Routing Information Protocol (RIP) version 1 & version 2
- Open Shortest Path First (OSPF)

Routing Information Protocol (RIP) is a distance vector routing protocol that can be used to automatically build the routing table in Windows 2000. A distance vector protocol means that the routing table consists of routes that are configured with a distance (hop count) and a vector (the gateway to the destination network). When RIP is installed on RRAS, the router begins to broadcast its internal routing table every 30 seconds. The router also receives broadcasts containing routing tables from other routers. In this way, each router builds a routing table that lists how to connect all of the networks.

The routing table is based on hop counts. The **hop count** is the number of routers that must be crossed to reach a destination network. A RIP router builds its routing table containing only the lowest hop count route to any network that it identifies during the process of building the routing table. One of the limitations of RIP is that it has a maximum hop count of 15; in other words, any network that is more than 15 routers away is listed as unreachable.

Another limitation of RIP is that it does not react very quickly to failed routes. If a RIP router does not receive any update packets from an adjoining router, it waits for three minutes before listing the route as unavailable. The RIP router only then begins the process of informing other routers that the route is down. RIP has been modified to be more efficient by triggering updates. This means that if a router detects an unavailable route, it immediately informs the other routers and does not wait for the next scheduled update.

Open Shortest Path First (OSPF) is a link-state routing protocol that is well suited for larger networks. A link-state router builds a routing table that includes the entire local network, as well as links to external networks. Each router maintains a database that contains the topology of the entire network from the router's perspective.

OSPF scales better than RIP in large networks. Because each router has an overview of the entire network, the routers can make more intelligent decisions for routing rather than basing the routing table only on hop counts. In addition, OSPF routers more quickly detect downed routers and propagate the changes to other routers. OSPF also supports variable length subnet masks, authentication, and more control of the size of the routing table. OSPF allows you to control what parts of the network will be stored as detailed routes and what parts of the network will be stored as summarized routes. The primary disadvantages of OSPF are that it is more difficult to configure, and it requires more processing by the router to calculate the routing database. Thus, more processing power is required on the router.

Configuring RRAS as a Demand-Dial Router

In addition to operating as a LAN-to-LAN router, Windows 2000 RRAS can also operate as a **demand-dial router**. In a demand-dial environment, at least one of the network connections to the server is not always connected, but the connection must be initiated by the server. A common example is a server where one of the network connections is a modem of some type, usually connected to the phone or ISDN line. When a packet arrives at the router that has a destination address in the network accessible through the dial-up connection, the RRAS server will initiate the connection to the remote network. In addition, the RRAS server can act as a demand-dial VPN router, in which an encrypted tunnel is created through the Internet between two or more corporate locations only when a packet destined for the other network is received by the RRAS server.

To configure the RRAS server to operate as a demand-dial router follow the steps below:

1. Click **Routing and Remote Access** from the **Administrative tools** menu. The RRAS console is shown in Figure 9-8.

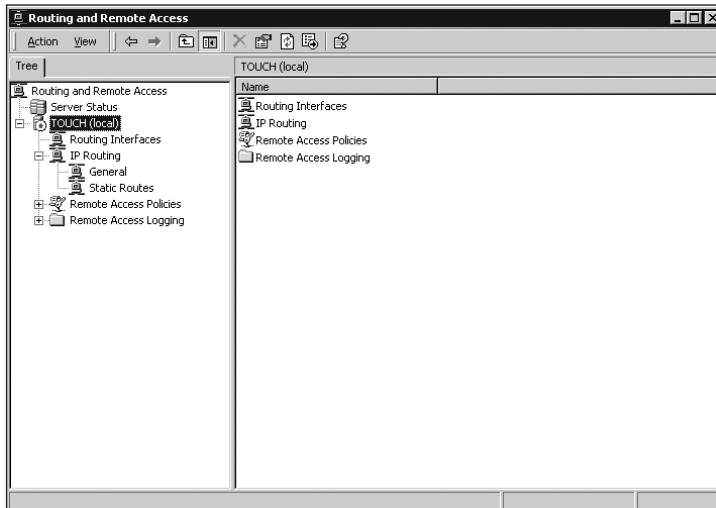


Figure 9-8 Configuring demand-dial routing in the RRAS console

2. Right-click the server name and click **Properties**.
3. Make sure that the Router check box is selected. Choose the **LAN and demand-dial routing** radio button as shown in Figure 9-9.

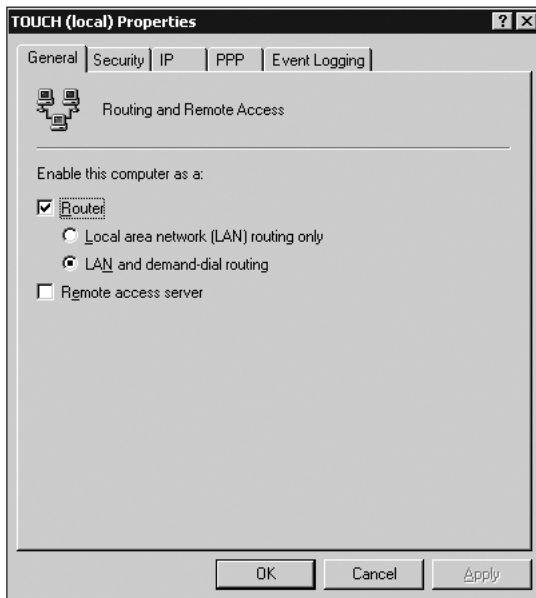


Figure 9-9 Configuring router options

4. RRAS may restart, and then add ports that can be used for the remote access connections, such as VPN and modem ports. Figure 9-10 shows the Ports node selected.

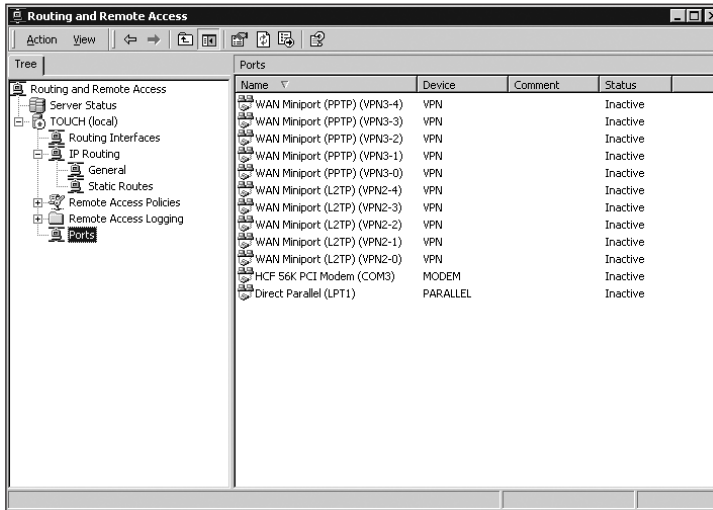


Figure 9-10 Viewing the RRAS ports

Demand-dial router interfaces can be configured when the cost of maintaining a permanent wide area network connection becomes a concern. Dial-up connections can be configured between the routers and can incorporate specific features, such as idle disconnect or permanent connection settings. The router connections can be authenticated by incorporating a router name and password into the Windows 2000 directory database and using this account during the dial-up configuration settings.

To configure a demand-dial router, a demand-dial interface must be configured in the RRAS console. This may have been set up during the initial RRAS configuration, but can also be configured separately as shown in the following procedure:

1. In the RRAS console, right-click **Routing Interfaces** and click **New Demand Dial Interface**. The Demand Dial Interface Wizard will appear. Click **Next**.
2. Type a descriptive name for the interface. For example, as shown in Figure 9-11, if this interface is a connection to Toronto, use a descriptive name that describes the connection such as **TORouter**. Click **Next**.
3. The next step is to choose the connection type. If you are using a physical device such as a modem, choose **Connect using modem, ISDN Adapter, or other physical device**. If you are creating a VPN connection between the two routers, choose **Connect using virtual private networking (VPN)**. (For this procedure, "Connect using modem..." will be chosen. VPN connections will be discussed in the next section of this chapter.) Click **Next**.

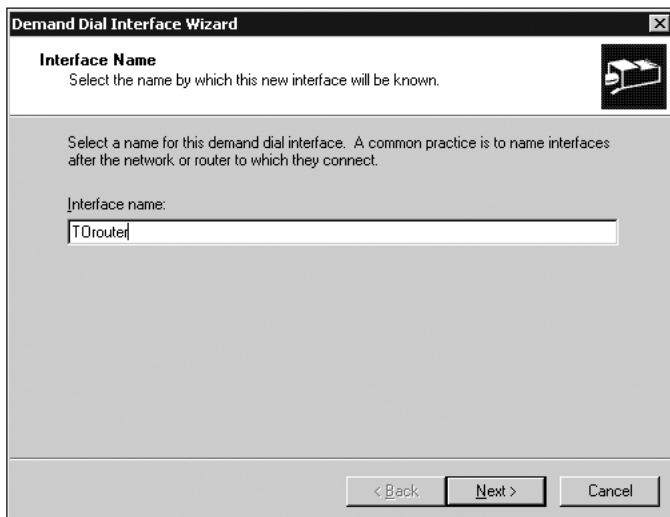


Figure 9-11 Configuring a demand dial interface name

4. The next step of the Wizard will allow you to choose the physical device to establish the connection. See Figure 9-12. Click **Next**.

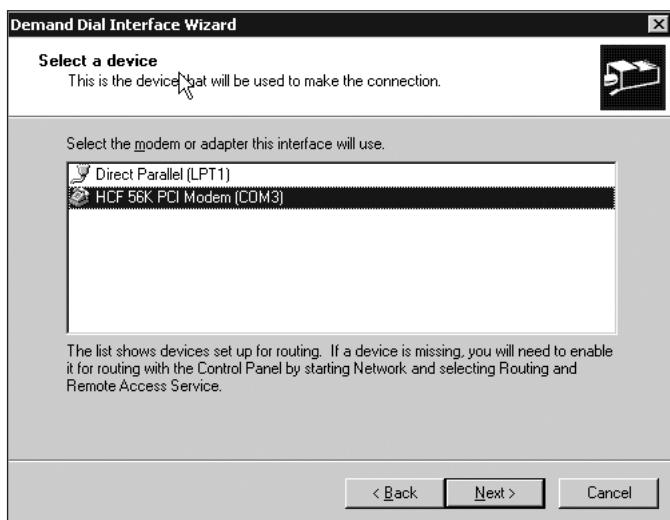


Figure 9-12 Choosing a modem as the demand dial interface

5. Enter the phone number of the remote server or router. Alternate numbers can also be configured by clicking the **Alternates** button. Click **Next**.

6. As shown in Figure 9-13, the Protocols and Security dialog box now appears. Select the type of packets (IP or IPX) that are to be used over this router connection. If the remote router is able to dial into this router, choose **Add a user account so a remote router can dial in** so that the remote router can authenticate to the local router.

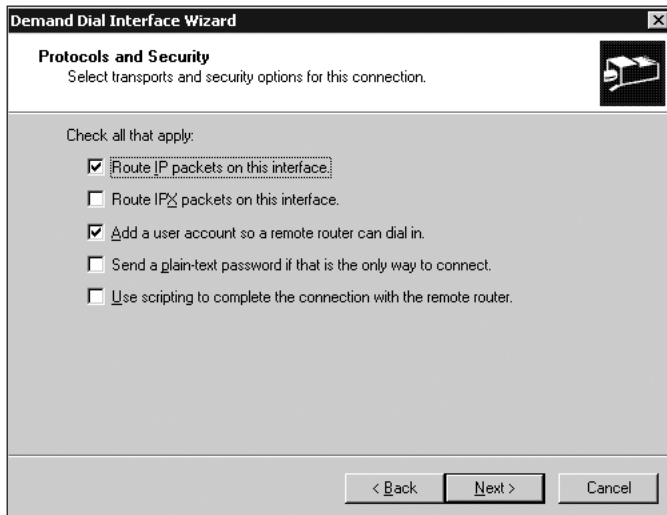
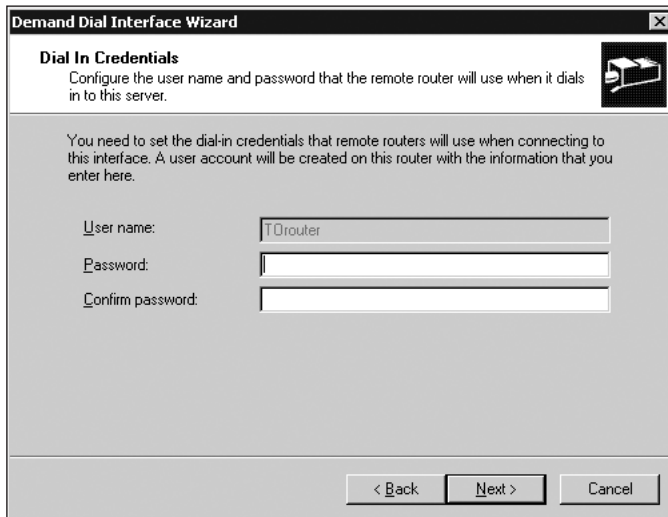


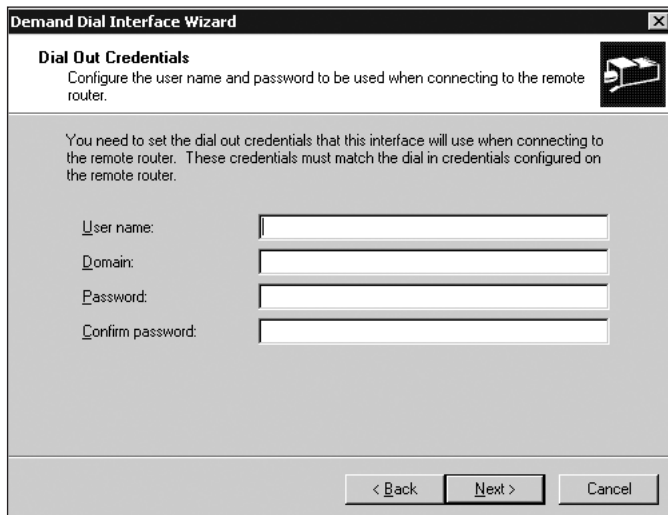
Figure 9-13 Options available in the Protocols and Security dialog box

7. If **Add a user account so a remote router can dial in** is selected, the next step, as shown in Figure 9-14, is to create the password for the new user. This user will be created in the directory database. (On a standalone server, this account is created in the local directory; if the RRAS server is a member of a domain, the account is created in the domain database.)
8. The next step in the Demand Dial Interface Wizard requires the configuration of the dial out credentials. The dial out credentials of the calling router must match the interface name of the demand-dial interface on the router being called. An illustration of this screen is shown in Figure 9-15.



The screenshot shows the 'Demand Dial Interface Wizard' window, specifically the 'Dial In Credentials' step. The window title is 'Demand Dial Interface Wizard'. The subtitle is 'Dial In Credentials'. Below the subtitle, it says 'Configure the user name and password that the remote router will use when it dials in to this server.' There is a small icon of a computer with a dial-up cable. The main text says 'You need to set the dial-in credentials that remote routers will use when connecting to this interface. A user account will be created on this router with the information that you enter here.' There are three input fields: 'User name:' with the text 'T0router', 'Password:', and 'Confirm password:'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 9-14 Setting dial-in credentials for the remote router



The screenshot shows the 'Demand Dial Interface Wizard' window, specifically the 'Dial Out Credentials' step. The window title is 'Demand Dial Interface Wizard'. The subtitle is 'Dial Out Credentials'. Below the subtitle, it says 'Configure the user name and password to be used when connecting to the remote router.' There is a small icon of a computer with a dial-up cable. The main text says 'You need to set the dial out credentials that this interface will use when connecting to the remote router. These credentials must match the dial in credentials configured on the remote router.' There are four input fields: 'User name:', 'Domain:', 'Password:', and 'Confirm password:'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 9-15 Configuring dial out credentials

9. Click **Finish** to end the Demand Dial Interface Wizard.

The final step in configuring a demand-dial router connection is to add static routes to the routing table for all of the remote networks that you will be connecting to using the demand-dial link. The procedure to add the static routes is the same as discussed in the LAN-to-LAN configurations section.

Securing the Windows 2000 Router

The Windows 2000 implementation of RRAS is a full-featured software-based router. RRAS also includes several security options that can be used to enhance the security of the transmission of packets as the data is routed throughout the network. These security features include packet filtering, mutual authentication, and encryption.

Packet filtering is the first and most important security option. **Packet filtering** consists of setting rules and conditions on how packets are sent and received on a network. Routers can be configured so that only certain types of packets will be forwarded through the router to a particular network segment. Most routers, including Windows 2000 RRAS, allow you to create rules that control packets based upon user, network identification, protocol, or port.

This is an essential feature for any router, especially a router that is exposed to the Internet. The role of a router is to forward packets from one network to another. If the router is attached to the Internet, this creates a serious security breach because the router will, by default, accept any packet from the Internet and forward it to the internal network. If you do not change this default, all an attacker has to do is learn the internal IP address of your network, and they will be able to send any packets into your internal network. Packet filtering is one of the ways to prevent this. For example, if you are using RRAS to create a VPN tunnel through the Internet, you can configure a packet filter so that the router will accept and forward only Point-to-Point Tunneling Protocol (PPTP) packets that come from the IP address of the router at the other end of the VPN tunnel. All other packets will be discarded.

To create a packet filter follow the procedure below:

1. Click Routing and Remote Access from the Administrative tools menu.
2. Expand the server container and then expand **IP Routing**. Click the **General** node.
3. In the right pane, right-click the interface that is to have the packet filter applied and click **Properties**.
4. The Network Properties dialog box will appear as shown in Figure 9-16.
5. Choose the **Input Filters** to filter traffic that is coming into this network interface or **Output Filters** to filter traffic that is being sent out of the network interface.
6. As illustrated in Figure 9-17, you can use the Input or Output Filters dialog box to add filters that can accept or reject network packets based on attributes such as source or destination address and source or destination protocol.

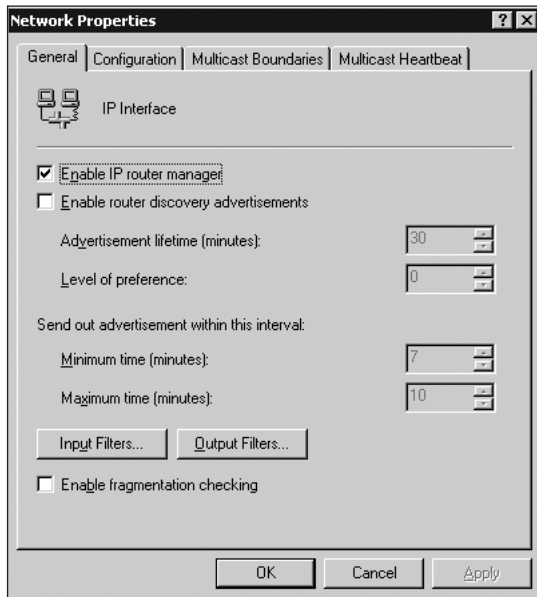


Figure 9-16 Configuring a router-based packet filter

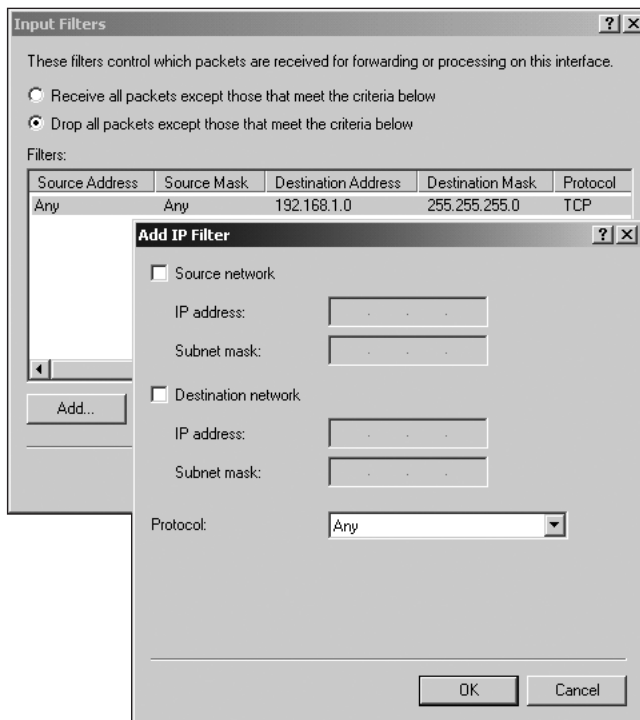


Figure 9-17 Configuring an input filter

You can also use packet filtering to filter packets that are sent through a demand-dial interface. This is important if you want to limit what types of packets can initialize a demand-dial connection to the remote router. To create a demand-dial filter, follow the steps below:

1. In the Routing and Remote Access Console, expand the server container and click the **Routing Interfaces** node.
2. Right-click the demand-dial interface and choose **Set Demand-dial Filters**.
3. A filter configuration screen identical to the one shown in Figure 9-17 appears, allowing the addition, deletion, or modification of demand-dial filters.

Mutual authentication is a second option that can be used to enhance the security of RRAS routing. Mutual authentication can be used as part of a demand-dial configuration to prevent an unauthorized router from establishing a connection to a router on a company's private network. The router on the private network can be configured to transmit packets only to external routers that have been authenticated. As discussed previously, a demand-dial router connection authenticates by supplying a username and password assigned to the router interface. To configure the authentication credentials for a demand-dial connection, follow the steps below:

1. In the RRAS console, select the **Routing Interfaces** node.
2. Right-click the **demand-dial interface** and choose **Set Credentials**.
3. Enter the credentials needed to dial-up successfully to the remote router connection. The Interface Credentials dialog box is shown in Figure 9-18.

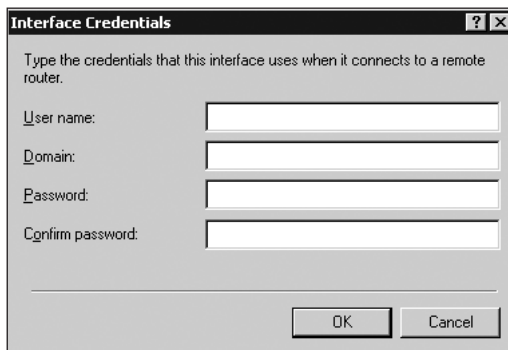


Figure 9-18 Setting remote dial-up credentials

Encryption guarantees that any transmission of information over the WAN link is confidential, and cannot be viewed if captured between the two encrypted points. For demand-dial router connections, standard dial-up encryption and authentication protocols can be implemented, such as MS-CHAP, MS-CHAP version 2, and EAP. To configure the authentication and encryption protocol for demand-dial routers, follow the procedure below:

1. In the RRAS console, select the **Routing Interfaces** node.

2. Right-click the demand-dial interface and choose **Properties**.
3. Click the **Security** tab (shown in Figure 9-19) and choose the desired security settings.

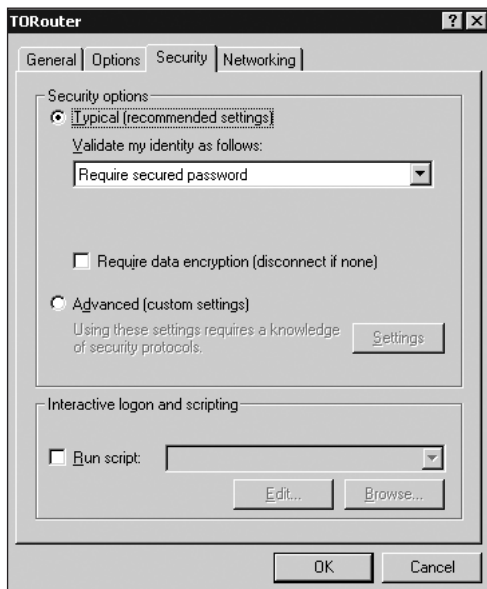


Figure 9-19 Configuring security settings for demand-dial routing

Another important security option is to use VPNs. When you use VPNs to route traffic between routers, all of the network traffic is protected by VPN protocols, such as PPTP and L2TP. These protocols secure the traffic by encrypting and authenticating packets as they are transmitted to the remote connection. Setting up virtual private networks is discussed in the next section of this chapter.

CONFIGURING AND SECURING VIRTUAL PRIVATE NETWORKS

Another option to secure traffic flowing between routers in remote networks is to use a **virtual private network (VPN)**, which creates a virtual network through an existing network by encapsulating and encrypting all the packets being transmitted between two remote routers. A VPN creates a virtual “tunnel” that protects data as it is transmitted over an unsecured network such as the Internet. VPNs are quickly gaining popularity because of their ease of use and security benefits.

One of the ways that a VPN can be utilized is to solve the limitations of dial-up networking over the regular phone lines. If you are supporting direct dial-up RAS connections to the corporate network, you will have to maintain a bank of modems and

phone lines to accommodate incoming connections. This can be expensive, since it is difficult to effectively balance the number of users with the phone line and modem resources. The connection speeds are limited by the capability of the phone lines, which are usually limited to 56 Kbps at best. In addition, the cost of having all of the remote users call long distance numbers can be prohibitive.

There are many scenarios where VPN technology can assist a corporation. For example, Lonestar Graphics may have employees who travel extensively and who need access to the company network from anywhere. In the past, Lonestar Graphics might have utilized Remote Access Services (RAS) to allow remote users to dial into the network using a modem. This was quite expensive, as users had to dial long distance and incur phone charges to connect to the network. There was also a limitation on the number of users that could dial in, because of hardware restrictions. If the company had only two dial-up modems available for remote users, only two users could connect at one time.

VPN technology can assist Lonestar Graphics by decreasing costs and increasing functionality. First of all, users can be assigned user accounts with an ISP that covers the area where the remote users travel. This means that the users can dial local phone numbers to access the Internet, thus saving on long distance charges. After the users have connected to the Internet, they can create a VPN connection to the company's VPN server. This provides secure authenticated and encrypted transmissions between the user and the corporate network. This option also deals with the hardware limitation: one VPN server can handle hundreds of VPN connections at one time.

Remote offices can also take advantage of VPN technology. The cost of maintaining a dedicated link or having the remote office dial-up to the central office can be significant. By using a VPN, remote offices can take advantage of local ISP connections to the Internet. In many locations, the remote offices could be connected to the Internet through cable modem or DSL connections, which provide permanent and fast Internet connections at a reasonable cost. Setting up a VPN in this case is even easier than using a dial-up connection because the connection to the Internet is permanently available. All that needs to be configured is the VPN connection to the corporate VPN server.

VPN Tunneling Protocol Options

Windows 2000 virtual private networking supports three tunneling protocols. These protocols provide authentication and encryption features to ensure the secure transmission of packets over a public or private network. The three VPN protocol options include:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP) over IPSec
- IPSec Tunnel mode

The choice of which protocol to use over a VPN connection depends largely upon the network configuration and security needs of the organization.

Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP) is a VPN protocol developed by Microsoft with the collaboration of various third-party router manufacturers. To create a VPN connection using PPTP, the user connects to the VPN server and enters a username and password for authentication. The server and the client computer then use the authentication information to create a session key that is used to encrypt every packet that is sent across the public Internet, thus creating a tunnel of encryption through the Internet.

PPTP uses **Microsoft Point-to-Point Encryption (MPPE)** to encrypt the data. However, before the data can be encrypted using MPPE, the user must be authenticated using either MS-CHAP (version 1 or 2) or EAP-TLS (Extensible Authentication Protocol-Transport Level Security). Encryption with MPPE is considered to be link-to-link encryption, or client-to-server encryption. This means that packets are encrypted from the client to the VPN server, but any transmissions beyond the VPN server into the LAN are not encrypted.

Once the user has been authenticated, a PPTP control connection is created between the client and the server using TCP port 1723. This control connection is used to establish and maintain the PPTP session between the two computers. Another purpose for the control connection is to determine the highest possible level of encryption supported by both the client and the server.

After the PPTP control connection has been established, the actual transmission of data begins:

1. The data that is being transmitted is first encapsulated in a Point-to-Point (PPP) frame, which is then encrypted. MPPE, which uses the RSA RC4 encryption scheme and a 40-bit, 56-bit, or a 128-bit secret key, is used to encrypt the data. The keys used for the encryption are generated during the authentication process and are based on the shared secret (password) exchanged during the authentication process. PPTP supports the encryption of TCP/IP, NetBEUI, and NWLink packets.
2. The encrypted PPP frame is encapsulated in a modified **Generic Routing Encapsulation (GRE)** packet. GRE is an IP protocol with a protocol number of 47.
3. The GRE-PPP encapsulated packet is then further encapsulated into an IP packet. The IP packet contains a header that includes source and destination addresses of the PPTP client and server.
4. The final encapsulation occurs when the packet is sent to the data-link layer where the data-link header and trailer are added to the packet. The packet is then forwarded onto the network.

Figure 9-20 illustrates the encapsulated packet.

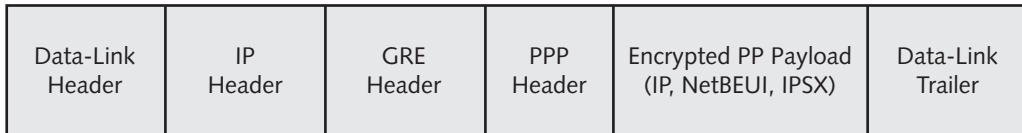


Figure 9-20 PPTP encapsulation structure

When the packet arrives at the PPTP server, the following steps occur:

1. The data-link information is removed from the packet.
2. The IP address is checked and the header is removed.
3. The GRE and PPP headers are removed.
4. The PPP payload is decrypted using the session key created during the authentication process, and the destination address for the payload is checked. If the packet was intended for the RAS server, it will be processed by that server; if it was intended for another server on the LAN, the packet will be forwarded.

PPTP can best be implemented when:

- Network clients use operating systems such as Windows 9x, Windows NT, and Windows 2000.
- The VPN connection crosses a firewall or router performing Network Address Translation (NAT). NAT modifies the IP address and port information in an IP packet. The fields that are modified by NAT are not protected by the MPPE encryption process, so PPTP can be used through a NAT server.
- Authentication of computer accounts is not a requirement. PPTP only supports user-based authentication.
- When network hardware does not support L2TP/IPSec.



To allow PPTP packets to pass through a firewall, TCP port 1723 and protocol ID 47, which is the GRE protocol, must be open.

Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) is a VPN protocol that incorporates technologies derived from Microsoft's PPTP and Cisco's Layer 2 Forwarding (L2F) tunneling protocols. Just like PPTP, L2TP can be used to secure transmissions between client and server, or router-to-router connections. L2TP provides functions similar to PPTP in that it is used to create a tunnel through the Internet and provide user authentication through dial-up authentication protocols. The major difference between PPTP and L2TP is that L2TP does not include any encryption method. L2TP only creates a tunnel through a

public network. To provide encryption, and to provide the additional benefit of computer authentication, IPSec is automatically used to negotiate a security association and encrypt the data between the two points of the L2TP tunnel.

When a client connects to an L2TP VPN server, the client is authenticated using any of the typical dial-up authentication options. Because L2TP uses IPSec to encrypt the data, any of the authentication methods can be used to achieve secure access to the server.



To allow the IPSec packets to pass through a firewall, User Datagram Protocol (UDP) port 500 and protocol ID 50, which is the IPSec Encapsulating Security Payload (ESP) protocol, must be open.

L2TP is similar to PPTP in many ways. As with PPTP, the first step in making an L2TP connection is to make a control connection that is used to create and maintain the tunnel between the two computers. After the L2TP control connection has been established, the actual transmission of data begins. Like PPTP, L2TP also supports TCP/IP, NetBEUI, and NWLink; the packet can use any of these protocols. The L2TP encapsulation process is outlined in the following steps:

1. The data that is being transmitted is first encapsulated in a PPP packet, which is then encapsulated in an L2TP packet.
2. The L2TP packet is encapsulated in a UDP packet.
3. The UDP packet is encrypted and encapsulated with an IPSec ESP and/or AH header and trailer.
4. The entire IPSec packet is encapsulated in an IP packet containing the source and destination IP address of the VPN client and server.
5. The IP packet is then encapsulated with a header and trailer for the data-link interface.

The entire L2TP/IPSec packet is depicted in Figure 9-21.

Data-Link Header	IP Header	IPSec Header	UDP Header	L2TP Header	PPP Header	PPP Payload (IP, NetBEUI, IPX)	IPSec Trailer	Data-Link Trailer
------------------	-----------	--------------	------------	-------------	------------	--------------------------------	---------------	-------------------

Figure 9-21 L2TP/IPSec encapsulation structure

One of the problems with using the L2TP protocol is that it cannot pass through a firewall that is configured to use NAT. IPSec encryption protects the IP address and port information. When the packet is received at the tunnel end point, it is discarded because the addressing information of the packet has been modified by the NAT protocol.

L2TP has two other important disadvantages when compared to PPTP. First, L2TP/IPSec is supported only if both the clients and server are running Windows 2000. The second disadvantage is the way in which IPSec is implemented. To gain maximum benefit, IPSec requires that both the server and the client have security certificates because the keys used to encrypt and decrypt the data come from the certificates. This means that all of the client computers and servers need to install the correct certificates. You can use the Certificate Server provided with Windows 2000 Server to assign the certificates to all of the clients, but this adds a great deal of administrative complexity.

IPSec Tunnel Mode

As discussed in Chapter 7, IPSec can be used to encrypt packets as they are transmitted across a network connection. IPSec can be used in two different modes: Transport mode and Tunnel mode. Tunnel mode uses ESP to encrypt all traffic between the two tunnel end-points. Consider the following points when deciding on IPSec Tunnel mode:

- IPSec provides only machine authentication between the tunnel end-points, not from the client computer to the destination computer.
- IPSec cannot be used if you are using Network Address Translation (NAT).
- IPSec tunnel mode is supported by more routers and third-party hardware devices than L2TP with IPSec. That means that you can use a Windows 2000 RRAS server as one end-point of an IPSec tunnel and a third party hardware router as the other end-point.

CONFIGURING SECURE ACCESS TO PARTNER ORGANIZATIONS

Most of the concepts covered in this chapter so far have dealt with ways to secure network traffic that is flowing between multiple locations in the same corporation. However, many businesses are now forming temporary or long-term partnerships with other companies. In many cases, this partnership requires that some of the information on a company's network must be made available to users from the other organization. With this increase in business-to-business (B2B) communication comes an increase in the need to provide secure and reliable transmissions with partner organizations. The security plan needs to address a number of concerns, including securing the data transmission, authenticating users, and controlling access to resources on the company network.

Securing Data Transmissions

When companies begin to collaborate and share information, the first concern is the security of the data transmission between the company locations. From a security perspective, this may prove to be challenging, as network architectures may be different between the companies. This may restrict the security solutions that can be used. The

corporate security policies may also be quite different in the organizations, which may affect the way security can be implemented for interaction between the companies.

The method used to secure the communication between corporations greatly depends on what is being shared on each side of the connection. If companies are sharing only Web-based information, simple solutions, such as implementing SSL on the Web server, may be all that is needed. If access to certain applications is being shared between companies, you may want to deploy Terminal Services. Terminal Services uses the Remote Desktop Protocol (RDP), which incorporates encryption within the transmission. As stated in Chapter 6, “Securing Network Services,” setting the high encryption level for the RDP sessions will provide encryption in both directions for the transmission, as well as 128-bit encryption if Windows 2000 Service Pack 2 or the high encryption pack is installed.

Another option in securing transmissions between trusted partners is to implement a VPN solution, as discussed previously in this chapter. Whether the VPN is implemented as a PPTP, L2TP, or IPSec Tunnel mode connection will depend greatly on the requirements and resources available at each location.

Securing Resource Access to the Company Network

Providing access to resources between partner networks requires some type of user authentication and assignment of permissions to the resource. One of the options that you can use is to configure a trust between the two corporate domains. This is often the best option if the relationship between the two organizations will continue for an extended period of time, and if you have to give access to resources, such as files on a file server. In this scenario, you can configure one-way, non-transitive trusts between the domain or domains in your organization and the domains in the other organization. Then you can use the standard means to provide access to resources while still maintaining strict security. The first level of protection is to be sure to use NTFS security on all internal data shares. Then you can create a security group that contains the external partner user accounts and assign access to resources to that group.

You can also limit access to the company network by placing the resources that need to be shared in a screened subnet or Demilitarized Zone (DMZ). A DMZ is separated from the rest of the internal network by one or more firewalls. (See Figure 9-22 for an example.) The advantage of using a DMZ is that if resources become compromised within the DMZ, the rest of the internal network is not affected. For more information regarding the implementation of DMZs see Chapter 10.

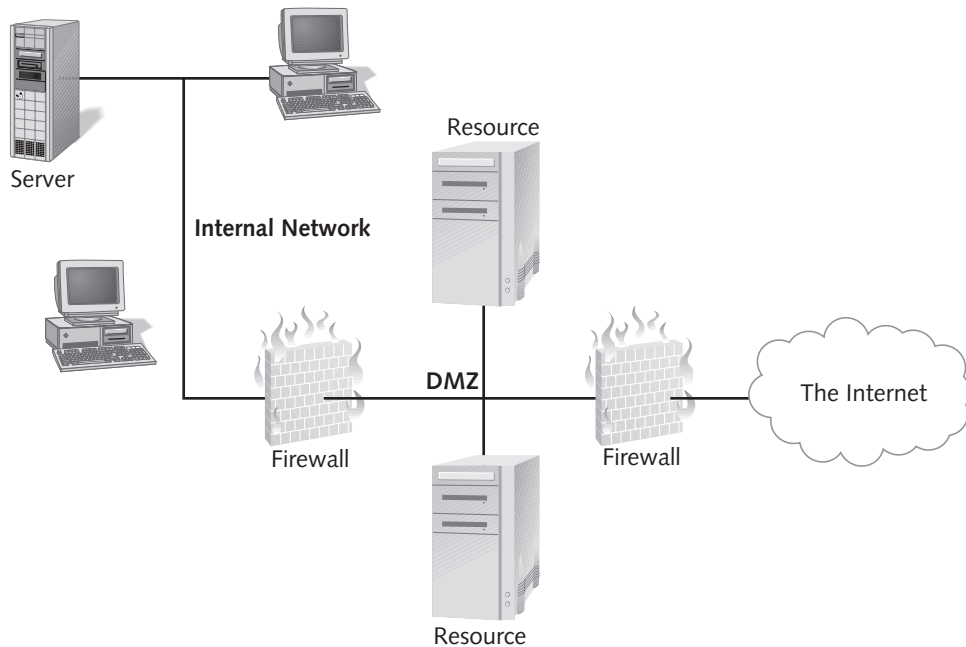


Figure 9-22 Securing resources within a DMZ

Another way of securing authentication and resource access is to take advantage of a Public Key Infrastructure (PKI). A PKI enables the authentication of external users who may not have an account in Active Directory. As long as users have obtained a certificate from a trusted certificate server or issuing service, you can use certificate mapping to control access to internal resources. The advantage of using certificate mapping is that a user account does not need to be created for each user that is going to be accessing the company network. Instead, you can create a single account in Active Directory, and then link the account to valid certificates.

As discussed in Chapter 5, there are two main ways to configure certificate mapping: one-to-one and many-to-one. One-to-one mapping associates a certificate to a corresponding user account in Active Directory. Many-to-one mapping links all of the certificates issued by a specific Certificate Authority to a corresponding user account in Active Directory. If you use the latter option, you can then assign access to your network resources to one user account, and all of the users who have a valid certificate will get access to the resources based on that one user account.

PLANNING BEST PRACTICES

- If you have numerous users dialing in to the corporate network from remote locations, the use of VPN connections rather than direct dial-up connections can provide significant savings for the organization. The disadvantage to using VPNs in this case is that it makes the configuration of the client computers slightly more complicated because you have to configure both a dial-up connection to an ISP and a VPN connection.
- If remote users are dialing in from many different locations, you can work with a national or international ISP to use a local access number for each of the locations.
- To provide the highest level of network security, use the strongest level of encryption supported by your clients. When the VPN connection is set up, the server and client will always negotiate to the highest level of encryption supported by both computers.
- One of the most important steps in configuring VPN connections between corporate locations is to configure packet filtering. If you do not configure packet filtering, attackers will be able to easily access your network.
- Configuring the packet filters can be complex, especially if you have to allow traffic on multiple ports or protocols. This can happen if users on the Internet need to get access to many different applications in your network. In this situation, you have to plan your packet filtering carefully and test your implementation thoroughly before putting it into production.
- Cable modems and DSL connections provide fast and inexpensive access to the Internet. Many companies are taking advantage of this to use the Internet as the WAN connection between corporate locations. If you are planning on using the Internet in this way, remember that the information that is sent on the Internet is not secure. You must secure confidential data using a VPN solution.
- Windows 2000 RRAS is a full-featured router, but it cannot provide all of the functionality and performance of a dedicated hardware router.

CHAPTER SUMMARY

- Wide Area Networks (WANs) can be implemented over private or public networks that permanently connect two or more remote locations within an organization.
- Some common security risks associated with connecting remote locations over a WAN link include data integrity, data confidentiality, and resource authentication.
- Routing and Remote Access Services (RRAS) can be implemented to provide services such as persistent or demand-dial router support, VPN support, RADIUS Client Support, and NAT.

- Windows 2000 can be implemented as a functional router that has the capability to route packets within a LAN or across a WAN connection. If you configure RRAS as a demand-dial router, it will connect to a remote location only when needed.
- To increase security, Windows 2000 router configurations provide packet filtering, mutual authentication, and encryption.
- Another option to secure router connections between remote networks is to use a Virtual Private Network. A Virtual Private Network (VPN) can be used to encapsulate and encrypt packets to provide security between two remote networks over a public network.
- Windows 2000 virtual private networking supports three types of tunneling protocols. These protocols provide authentication and encryption features to ensure the secure transmission of packets over a public or private network. The three VPN protocol options include PPTP, L2TP over IPSec, and IPSec Tunnel mode.
- Various areas of security have to be addressed when sharing information with partner organizations. Security of the data transmission can be addressed by utilizing protocols such as SSL/TLS and IPSec. VPN can also be implemented to provide a secure tunnel for data transmissions. User authentication and access to resources on the company network can be secured by incorporating Public Key Infrastructure, including certificate mapping.

KEY TERMS

demand-dial router — A router that initiates a dial-up connection to a remote location only when needed.

encryption — The process of scrambling data as it is transmitted between two points to ensure confidentiality.

Generic Routing Encapsulation (GRE) — The protocol used by PPTP to encapsulate the encrypted packets that are being transmitted across the Internet.

Layer 2 Tunneling Protocol (L2TP) — A protocol that provides authentication services over public networks. Often used in conjunction with IPSec to create secure VPN connections.

Microsoft Point-to-Point Encryption (MPPE) — The encryption algorithm used by PPTP to encrypt the packets before they are transmitted on the network. The keys used for the encryption are based on the user's name and password.

mutual authentication — The process of two points (routers) authenticating to each other to ensure that packets are sent only to authorized routers.

Open Shortest Path First (OSPF) — A link-state routing protocol where each router builds a routing table that includes the entire local network, as well as links to external networks.

packet filtering — Consists of setting rules and conditions on how packets are sent and received on a network.

Point-to-Point Tunneling Protocol (PPTP) — Network technology that gives clients using TCP/IP, IPX, or NetBEUI the ability to create a secure VPN over a public TCP/IP network, such as the Internet.

router — A networking device, either software-based or hardware-based, that controls and forwards packets between networks.

Routing and Remote Access Services (RRAS) — A Windows 2000 service that incorporates features such as dial-up access, routing, network address translation, and virtual private networking into a corporate network infrastructure.

Routing Information Protocol (RIP) — A distance vector routing protocol that can be used to automatically build the routing table in Windows 2000. A distance vector protocol means that the routing table consists of routes that are configured with a distance (hop count) and a vector (the gateway to the destination network).

routing protocols — Protocols used to automatically update the routing table entries.

routing table — A list of all the networks that a router has identified, and the addresses that the router can use to forward messages to that network.

static routes — Entries that have been manually entered into the routing table to assist the router in forwarding packets to networks not directly connected to the router.

virtual private network (VPN) — Used to encapsulate and encrypt packets to provide security between two remote networks over a public network.

wide area network (WAN) — A computer system that connects two or more remote locations over a wide geographical area.

REVIEW QUESTIONS

1. What type of encryption is used with L2TP for a Windows 2000 VPN?
 - a. MPPE
 - b. IPsec AH
 - c. IPsec ESP
 - d. none — L2TP provides its own encryption
2. Which VPN protocol can be routed through NAT?
 - a. PPTP
 - b. L2TP
 - c. neither
 - d. both
3. In order to use the Internet as a WAN connection between company locations you should:
 - a. use a VPN to secure the traffic
 - b. use only SMTP e-mail to send information through the Internet
 - c. configure your Web servers to use SSL
 - d. lease a dedicated connection such as a T1 line to the Internet

4. How can you allow VPN access for your clients but still be as secure as possible?
 - a. Place the VPN server behind a firewall on a screen subnet.
 - b. Be sure the VPN server is on a different subnet than client computers and internal servers.
 - c. Set up packet filters to allow only VPN packets to be routed to the server.
 - d. all of the above
5. A VPN can connect two networks using private IP address ranges across the Internet even though the Internet will not route the private IP address ranges. True or false?
6. The most important security-related advantage of a private WAN connection over a public WAN connection is that the private WAN is usually:
 - a. cheaper
 - b. faster
 - c. less accessible to other users
 - d. configured to automatically encrypt all network traffic
7. The easiest way to ensure that all traffic between a customer location and your Web server is secure is to:
 - a. Configure the Web server to use SSL.
 - b. Configure an L2TP tunnel from the customer location to the Web server.
 - c. Require each user from the customer location to log on to Active Directory before they get access to the Web site.
 - d. Configure the Web server to use digital signatures.
8. When you configure Windows 2000 RRAS as a router, you can configure the router to use a routing protocol. Which of the following is a routing protocol?
 - a. TCP/IP
 - b. IPX/SPX
 - c. OSPF
 - d. NetBEUI
9. Using a routing protocol is useful in a large company because:
 - a. You do not have to manually configure the routing tables.
 - b. You can assign different costs to routes between organizations.
 - c. You can send information between company locations.
 - d. You can use it to add static routes to the routing table.

10. The routing table on a router like RRAS includes what types of routes?
 - a. static routes
 - b. routes for all networks directly connected to the router
 - c. routes to the Internet
 - d. routes that have been added by routing protocols
11. The biggest disadvantage of using static routes is that:
 - a. Static routes do not include the fastest route between networks.
 - b. Static routes can easily be removed by router administrators.
 - c. Static routes cannot include networks other than those directly connected to the router.
 - d. Static routes do not automatically change for changing network conditions.
12. If you are planning to configure RRAS to use RIP, you should ensure that:
 - a. Your network does not have more than 15 hops to any location.
 - b. All the traffic between company locations will be encrypted using IPSec.
 - c. All the RRAS servers can calculate the link-state table.
 - d. Your network can route NetBEUI packets.
13. To configure RRAS as a demand-dial router, you need to:
 - a. Enable RRAS as a demand-dial router.
 - b. Configure the RRAS server to use OSPF.
 - c. Configure a static route for the demand-dial destination.
 - d. Configure a demand-dial interface.
14. When you configure packet filtering on the RRAS router, you are:
 - a. defining which network packets will be encrypted
 - b. defining which network packets will be blocked from entering the network
 - c. defining where network packets will be routed
 - d. defining the network packets that will be forwarded to another network
15. PPTP uses _____ to encrypt traffic sent through a VPN.
 - a. MPPE
 - b. IPSec AH
 - c. IPSec ESP
 - d. packet filtering
16. Which clients can be configured to use PPTP to create a VPN?
 - a. Windows ME
 - b. Windows NT 4.0

- c. Macintosh
 - d. Windows 2000
17. To configure a VPN connection using L2TP with IPSec, you will have to use:
- a. client and server certificates if the two computers are not in the same forest
 - b. Windows 98 or Windows 2000 client computers
 - c. a NAT device
 - d. only Windows 2000 clients

HANDS-ON PROJECTS



Project 9-1

In this hands-on project, you will configure Routing and Remote Access as a router.

To configure RRAS as a router:

1. Log on to your Windows 2000 computer as an administrator.
2. Click **Routing and Remote Access** from the Administrative tools menu.
3. Right-click the server name or click **Action** and click **Configure and Enable Routing and Remote Access**.
4. Click **Next** at the RRAS Setup Wizard welcome screen to view the common configurations of RRAS.
5. To configure the routing options, click **Network Router** and then click **Next**.
6. Verify that the required protocols are available. If they are not, you will have to cancel out of the Wizard and install the appropriate network protocols before continuing. Click **Next**.
7. The next screen allows the choice of configuring demand-dial routing. If configuring demand-dial routing, click **Yes**; otherwise click **No**, and then finish the Wizard.
8. If demand-dial routing is chosen, the next Wizard allows you to choose how IP addresses will be allocated. Click **Automatically**.
9. The final screen in the RRAS Setup Wizard lists additional configuration settings that should be completed after the wizard setup and before the server can be used as a router. Click **Finish**.
10. Continue with the next project.

9

Project 9-2

In this hands-on project, you will add a demand-dial interface to the router configuration created in the previous project. The demand-dial connection is to the Toronto branch office.

To add a demand-dial interface:

1. In the left pane, expand the RRAS server.
2. Click **Routing Interfaces**.
3. Right-click **Routing Interfaces** and choose **New Demand-dial Interface**. The Demand Dial Interface Wizard starts. Click **Next**.
4. Type **Toronto** for the Interface name.
5. For the **Connection Type**, choose to **Connect using virtual private networking (VPN)**. Click **Next**.
6. For the **VPN Type**, choose **Automatic selection**.
7. For the **Destination Address**, type **10.0.0.50**. Click **Next**.
8. On the **Protocols and Security** screen, check off **Route IP packets on this interface**. Click **Next**.
9. Fill in the following Dial Out Credentials:
 User Name: Lonestar
 Domain: Lonestar
 Password: password
 Confirm password: password
10. Click **Next** and **Finish**.
11. Continue to the next project.



Project 9-3

In this hands-on project, you will configure a static route that uses the dial-up RRAS connection when needed.

To view the routing table to see which routes are automatically configured:

1. Expand **IP Routing**.
2. Right-click **Static Routes**.
3. Click **Show IP Routing Table**. Notice that there is no route to the 10.0.0.0 network, which represents Toronto.
4. Close the Routing Table.
5. To create a static route to Toronto, right-click **Static Routes**.
6. Click **New Static Route**.
7. Choose **Toronto** for the Interface.
8. In the Destination box, type **10.0.0.0**.
9. In the Network mask box, type **255.255.255.0**.
10. Click **OK**.
11. Continue to the next project.



Project 9-4

In this hands-on project, you will secure the demand-dial VPN connection to Toronto.

To configure Router availability times:

1. Select **Routing Interfaces**.
2. Right-click the **Toronto** demand-dial interface.
3. Click **Dial-out Hours**.
4. Only permit dial-out hours Monday to Friday, 9 AM to 6 PM. Click **OK**.
5. To configure dial-up authentication protocols, right-click the **Toronto** demand-dial interface. Click **Properties**.
6. Click the **Security** tab.
7. Select the **Advanced** radio button and click **Settings**.
8. Only allow **MS-CHAP version 2** for the authentication protocol. Click **OK** twice.
9. Close all windows and log off.

CASE PROJECTS



Case Project 9-1

Many of the investors that own Southdale Property Management are investment companies. Some of these investment companies have asked for direct access into the Southdale Property Management network in order to access the most up-to-date information on the status of their investment. This request is currently being addressed by implementing a secure web site where the investors can log in and get access to the investment information. The problem is that the Web information is static and is updated only once a week, and some of the companies want daily updates. Because these investment companies have invested large amounts of money in Southdale Property Management, your management is telling you that you need to provide a solution for them. Evaluate the solutions that are available to you, and provide a recommendation for which solution to implement.



Case Project 9-2

The management at Fleetwood Credit Union is concerned about the high cost of the frame relay lines between the company locations. They are wondering if it would be possible to install a DSL connection at each office and use the Internet as a WAN connection between the offices. The biggest concern they have with this solution is security. The data sent across the Internet must be secure, and the users should still be required to connect through the WAN connection to head office to connect to the Internet. As well, the management wants to make sure that there is no way that an attacker can gain access to any of the offices through the Internet connection. Can this be implemented using Windows 2000 services? How would you set this up?

